I3T: Περιβάλλον Ευφυών Κτιρίων

Εργαλεία και Μηχανισμοί

Lidia Pocero Fraile, Απόστολος Φούρναρης και Χρήστος Κουλαμάς

Ινστιτούτο Βιομηχανικών Συστημάτων / Ε.Κ. «ΑΘΗΝΑ»

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΡΘΡΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ

ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

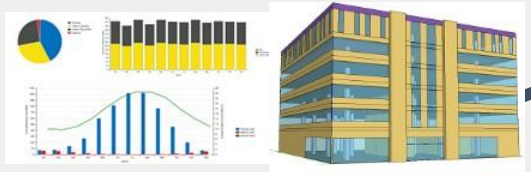
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ασφαλής Εγκατάσταση & Αρχικοποίηση

Ειδικές Απαιτήσεις και Ανοικτά Θέματα

- Ασύρματες IoT συσκευές με περιορισμένους πόρους
  - Χρήση βελτιστοποιημένων απλών μηχανισμών και πρωτοκόλλων
- Διαφορετικές εφαρμογές (φωτισμός, HVAC, ασφάλεια κλπ) πάνω από WSAN multi-hop τοπολογίες και υποδίκτυα διασυνδεδεμένα μέσω ενδιάμεσων πυλών που δεν ανήκουν απαραίτητα στην ίδια ζώνη εμπιστοσύνης
  - Ασφάλεια από άκρο σε άκρο σε επίπεδο εφαρμογής
- Αξιοποίηση ανοικτών προτύπων και ανοικτού λογισμικού

Υποδομή Ευφυών Κτιρίων I3T

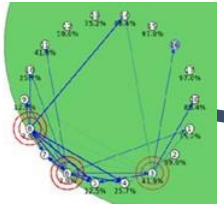


Εικονικά Περιβάλλοντα

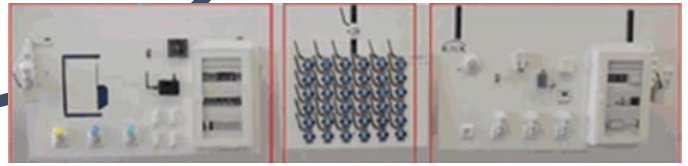
Συστήματα Παρακολούθησης & Διαχείρισης

Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

Εργαλεία Μοντελοποίησης Κατανάλωσης Ενέργειας

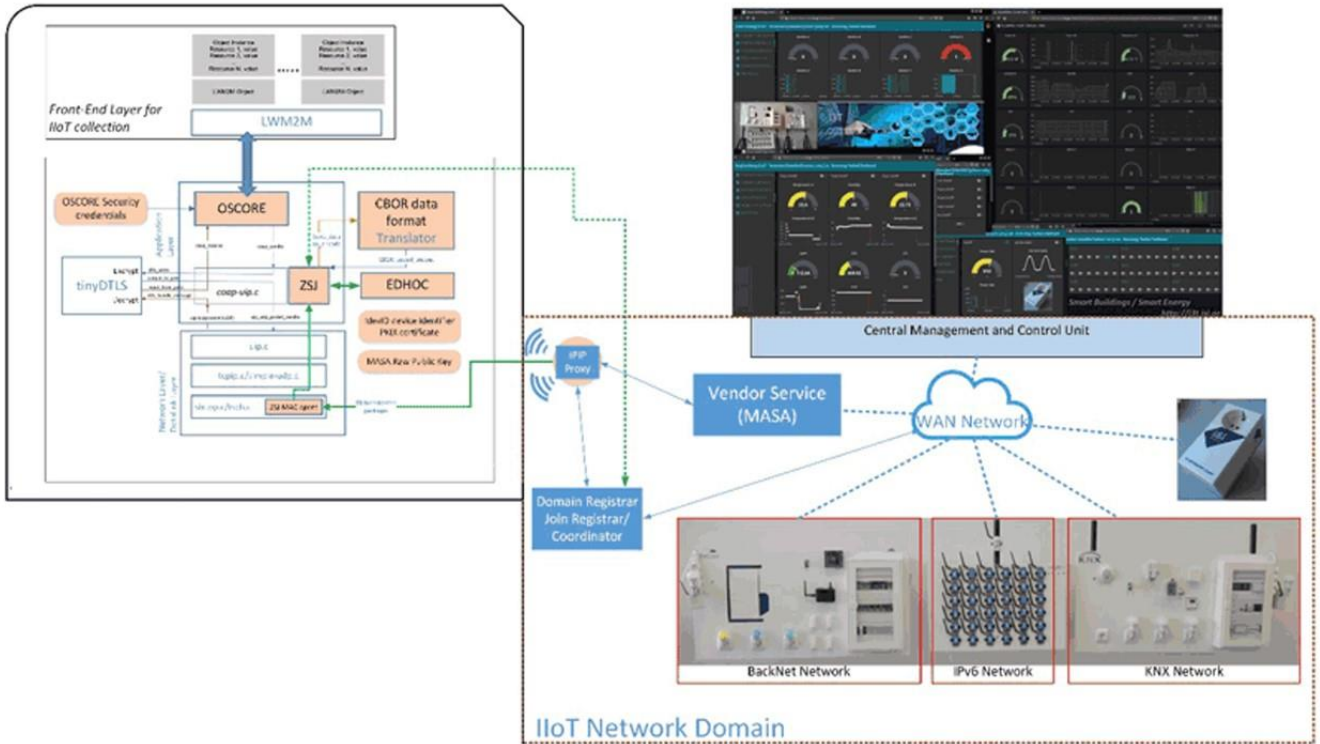


Εργαλεία Εξομοίωσης Ασύρματων Δικτύων Αισθητήρων



Ετερογενή Δικτυωμένα Συστήματα & Hardware in the Loop

Αρχιτεκτονική Συστήματος



EDHOC: Ephemeral Diffie-Hellman πάνω από COSE

IETF Draft [draft-ietf-edhoc-05]

Πιστοποιημένο πρωτόκολλο ανταλλαγής κλειδιών DH

Προορίζεται για χρήση σε σενάρια με περιορισμένους πόρους:

- Είναι πολύ συμπαγές και ελαφρύ
- Βελτιστοποιημένο με μηνύματα μικρού μεγέθους

Παρέχει αμοιβαίο έλεγχο ταυτότητας, από άκρο σε άκρο απόρρητο (forward secrecy) και προστασία ταυτότητας

Value	Initiator	Responder
0	Signature Key	Signature Key
1	Signature Key	Static DH Key
2	Static DH Key	Signature Key
3	Static DH Key	Static DH Key
4	PSK	PSK

Επαναχρησιμοποιεί:

- CBOR για κωδικοποίηση [RFC7049]
- COSE για κρυπτογράφηση [RFC8152]
- CoAP για τη μεταφορά [RFC7252]
- CoAP Block-Wise [RFC7959]
- AEAD για encryption [RFC5116]
- HKDF για παραγωγή κλειδιού [RFC5869]

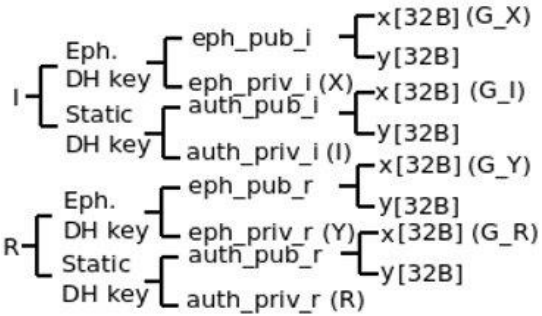
Name	Value	L	M	k	Description
AES-CCM-16-64-128	10	16	64	128	AES-CCM mode 128-bit key, 64-bit tag, 13-byte nonce

Value: 2
Array: 10, 5, 1, -7, 1, 10, 5
Desc: AES-CCM-16-64-128, SHA-256, P-256, ES256, P-256, AES-CCM-16-64-128, SHA-256

Τύποι Ελέγχου Ταυτότητας

Raw Public Keys (RPK)

- **PRK_ID**: περιέχει μόνο το Key ID
  - Τα μικρότερα μηνύματα
  - Προ-διαμοιρασμένο DH στατικό κλειδί



- **RPKI**: περιέχει το πραγματικό x στοιχείο του στατικού DH κλειδιού
  - Αρκετά μικρά μηνύματα

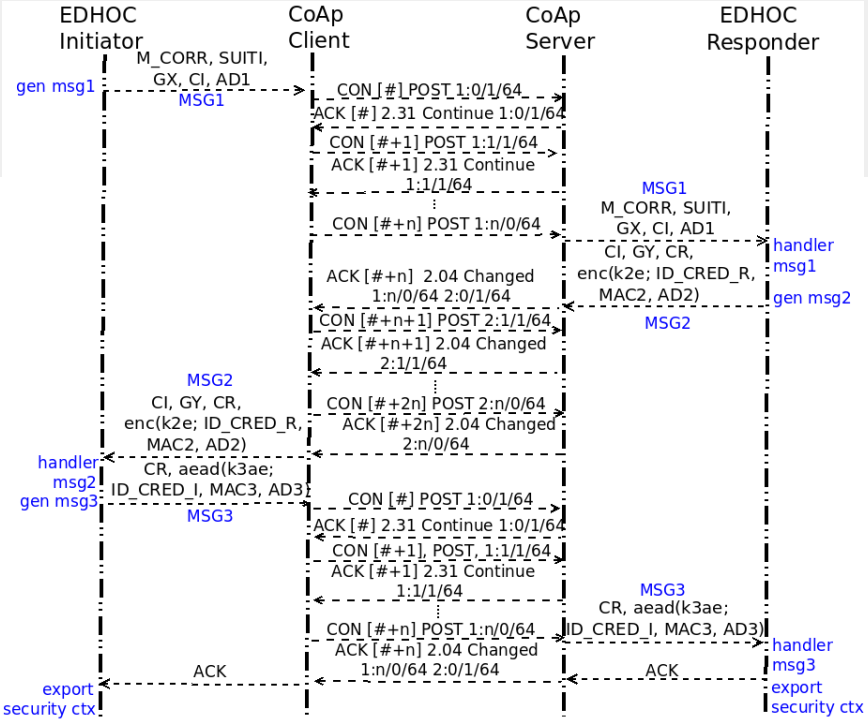
Public key certificates: X.509 certificates

- **X5T:** Η hash value 'x5t' χρησιμοποιείται για ταυτοποίηση του πιστοποιητικού.
  - Αρκετά μικρά μηνύματα
  - Το πιστοποιητικό X.509 είναι προ-διαμοιρασμένο

- **X5Chain**: DER κωδικοποίηση X.509 αλυσίδα πιστοποιητικών
  - Το μεγαλύτερο μήνυμα
  - X509 self-signed πιστοποιητικό

ATHENA Research & Innovation Information Technologies

Πρωτόκολλο Μεταφοράς



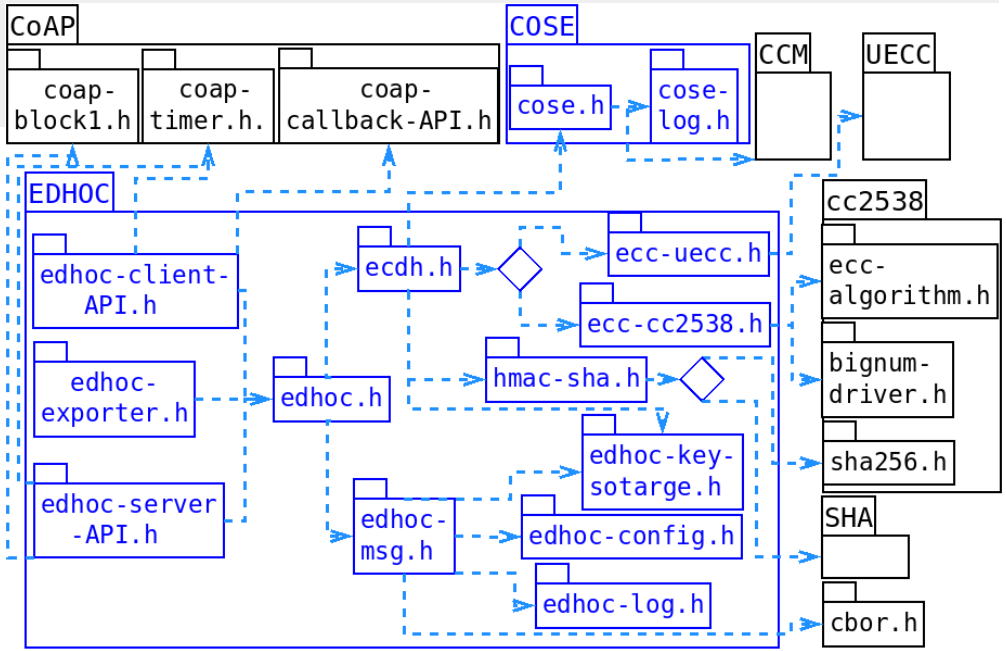
Contiki-NG Υλοποίηση

Δοκιμάστηκε με επιτυχία σε συνεδρίαση διαλειτουργικότητας (interoperability test) στο IETF 110 Hackathon.

Αίτημα σε εξέλιξη για merge στο επίσημο Contiki-NG.

Πλατφόρμα Περιορισμένων Πόρων: Zolertia ReMote

- TI's CC2538 SoC
- ARM Cortext-M3 CPU working up to 32MHz
- Programable flash: 512 Kbytes
- RAM: 32 Kbytes
- IEEE802.15.4 radio



ATHENA Research & Innovation Information Technologies

Αξιολόγηση Απόδοσης

	FUNCTION	OPERATIONS
(1)	new EDHOC ctx	ECDH key generate + key compress
(2)	generate MSG2	2 ECDH compute secret + 2 HKDF extract + 2 HKDF expand + XOR + SHA-256
(3)	handler MSG2	ECDH compute secret + HKDF extract + HKDF expand + XOR + SHA-256
(4)	generate MSG3	ECDH compute secret + 2 HKDF extract + 3 HKDF expand + SHA-256
(5)	handler MSG3	HKDF extract + 2 HKDF expand + SHA-256
(6)	authentication	ECDH compute shared secret + + HKDF extract + HKDF expand + SHA-256
(7)	export sec. ctx	SHA-256 + HKDF expand

Execution Time [ms]

OP.	HW drivers		ECDH SW		SHA SW	
	RPK_ID [ms]	RPKI [ms]	RPK_ID [ms]	RPKI [ms]	RPK_ID [ms]	RPKI [ms]
I (1)	341.4	344.8	540.6	541.4	344.0	351.0
R (1)	341.3	344.6	540.6	541.2	344.0	342.8
(2)	691.6	697.6	1168.8	1173.6	691.8	699.4
I (3)	342.4	350.0	582	589.4	344.8	350.4
(6)	347.6	350.1	583.6	583.8	348.4	348.8
(4)	346	347.0	589.6	591.0	346.8	347.0
R (5)	4.0	5.0	4.0	5.0	4.0	5.0
(6)	349.0	347.8	584.6	582.6	349.6	350.2
I / R (7)	5.0	6.0	5.0	5	5.0	6.0

Παράμετροι Αξιολόγησης:

- Χρόνος εκτέλεσης:
  - SW & HW EDHOC/SHA
  - 32 MHz & 16 MHz
  - Native Server & Constrained server
- Μέγεθος μηνύματος μεταφοράς
  - PRK_ID & PRKI Διαπιστευτήρια
- Αποτύπωμα (footprint) Μνήμης

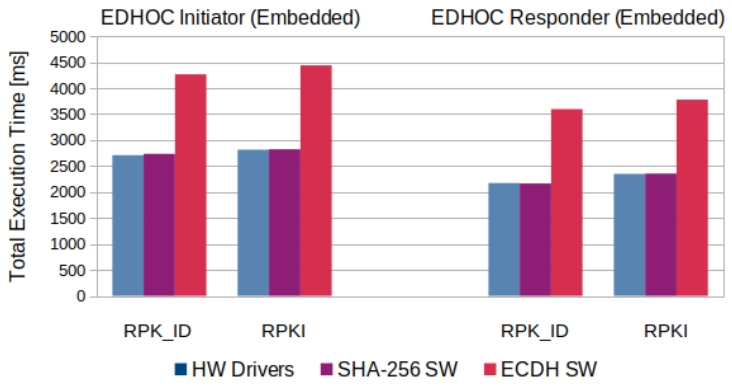
Βασικές πράξεις

- HKDF extract (SHA-256 op.)
- HKDF expand (Nº of SHA-256 ~ size)
- SHA-256 op.
- ECDH πράξεις (Δημιουργία κλειδιών και υπολογισμός κοινόχρηστου μυστικού)

ECDH op. αντιπροσωπεύει το μεγαλύτερο μέρος του χρόνου εκτέλεσης (95%)

ATHENA Research & Innovation Information Technologies

Αξιολόγηση Απόδοσης



	PRK_ID	PRK	X5T	X5CHAIN
MSG1	37 Bytes	37 Bytes	40 bytes	37 Bytes
MSG2	46 Bytes	135 Bytes	59 bytes	744 Bytes
MSG3	20 Bytes	109 Bytes	34 bytes	637 Bytes

Η επιτάγχυνση υλικού του ECDH:

- 36 % στον *Initiator*
- 37% με 40 % στον *Responder*

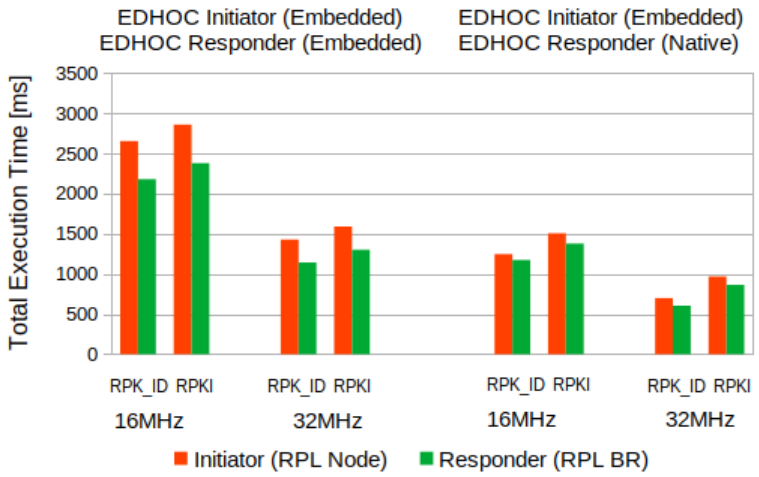
Η επιτάχυνση υλικού της λειτουργίας SHA-256 δεν παρουσιάζει σημαντικά πλεονεκτήματα

Η μέθοδος διαπίστευσης RPK_ID αύξησε τον συνολικό χρόνο εκτέλεσης από:

- 106 ms σε 172 ms στον Initiator
- 176.6 ms σε 192.2 ms στον Responder

ATHENA Research & Innovation Information Technologies

Αξιολόγηση Απόδοσης



	RAM			CODE SIZE	
	Overhead [KB]	Total [KB]	%	Overhead [KB]	Total [KB]
Initiator	5.8	20.3	63	13.1	62.2
Responder	5.7	20.6	64	8.4	61.4

Εγγυημένη εγκατάσταση κλειδιού σε:

- 2.8 sec (Constrains Devices στα 16 MHz)
- 0.9 sec (Constrains Devices στα 32 MHz)
- 1.2 sec (Responder runs native, Initiator στα 16MHz)
- 0.7 sec (Responder runs native, Initiator στα 32 MHz)

Πολύ μικρή επιβάρυνση ολόκληρου του δικτύου

Εγγυημένα αρκετά γρήγορη διαδικασία εγγραφής καινούργιων κόμβων

Είναι ικανό να τρέχει σε περιορισμένο μέγεθος RAM

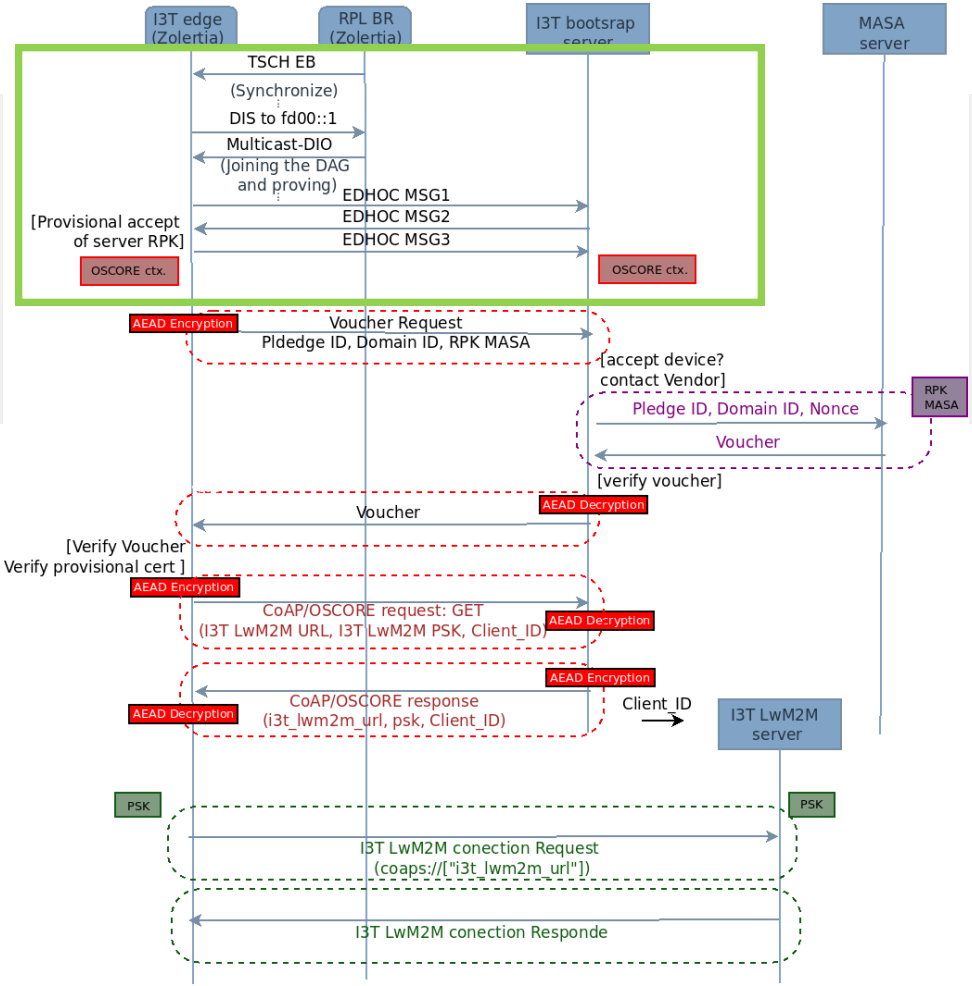
Αρχικοποίηση Ασφάλειας

Διαδικασία της αυτόματης εγκατάστασης νέου κόμβου

- Discover and Identify
- Request to Join
- Imprint
- Enrollment
- Done

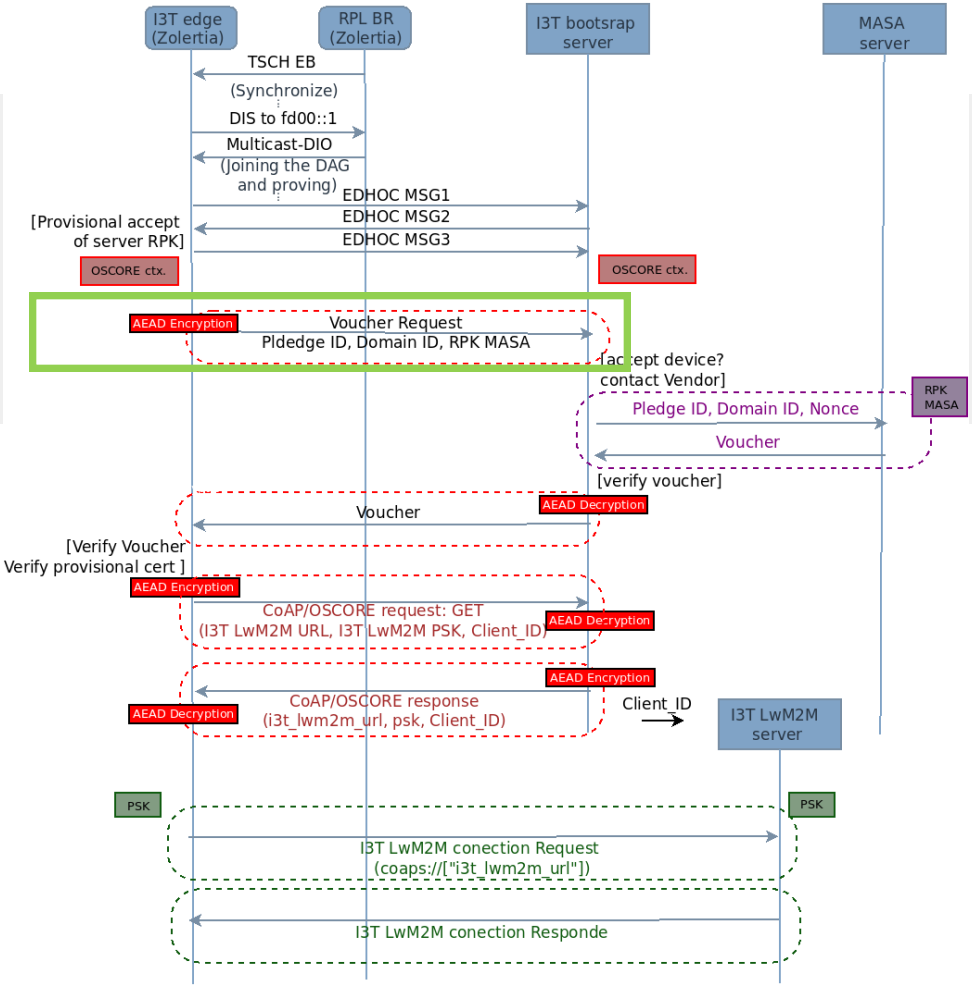
ATHENA Research & Innovation Information Technologies

1. Discover and Identify



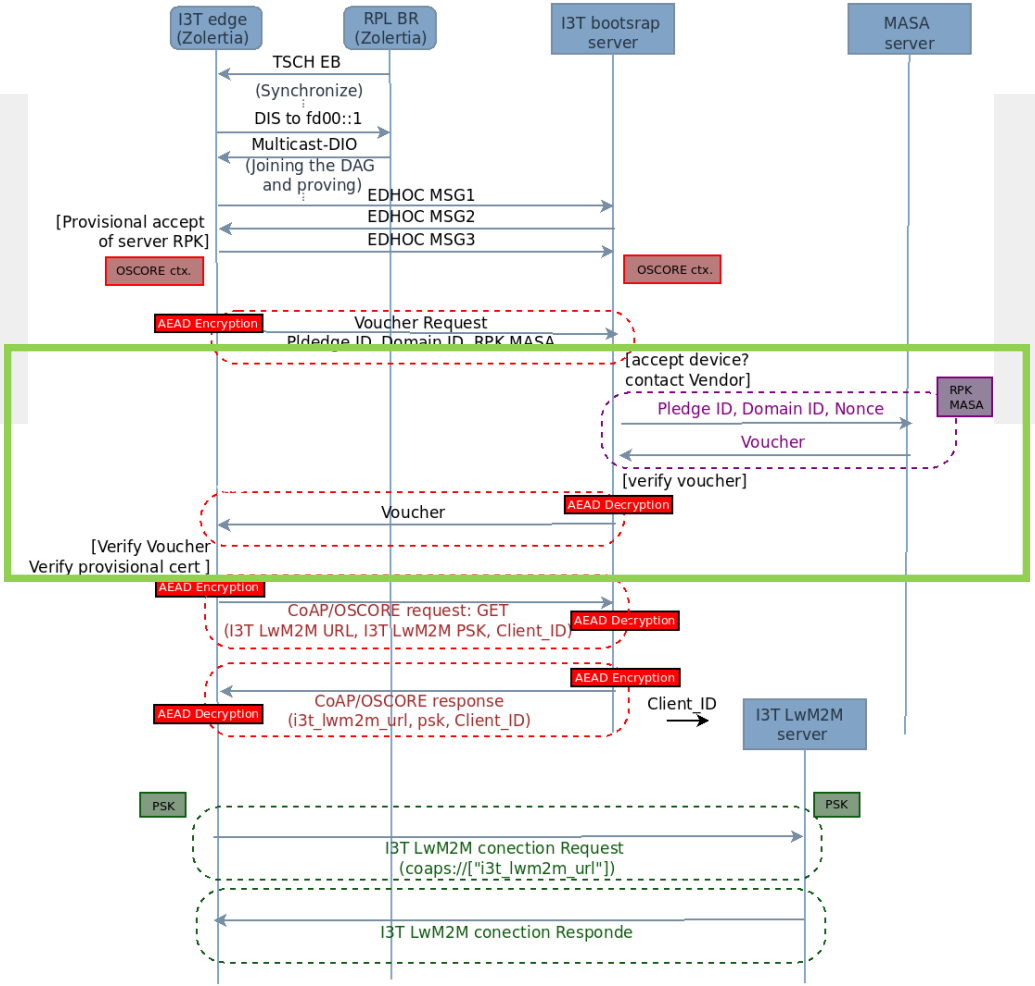
ATHENA Research & Innovation Information Technologies

2. Request to Join



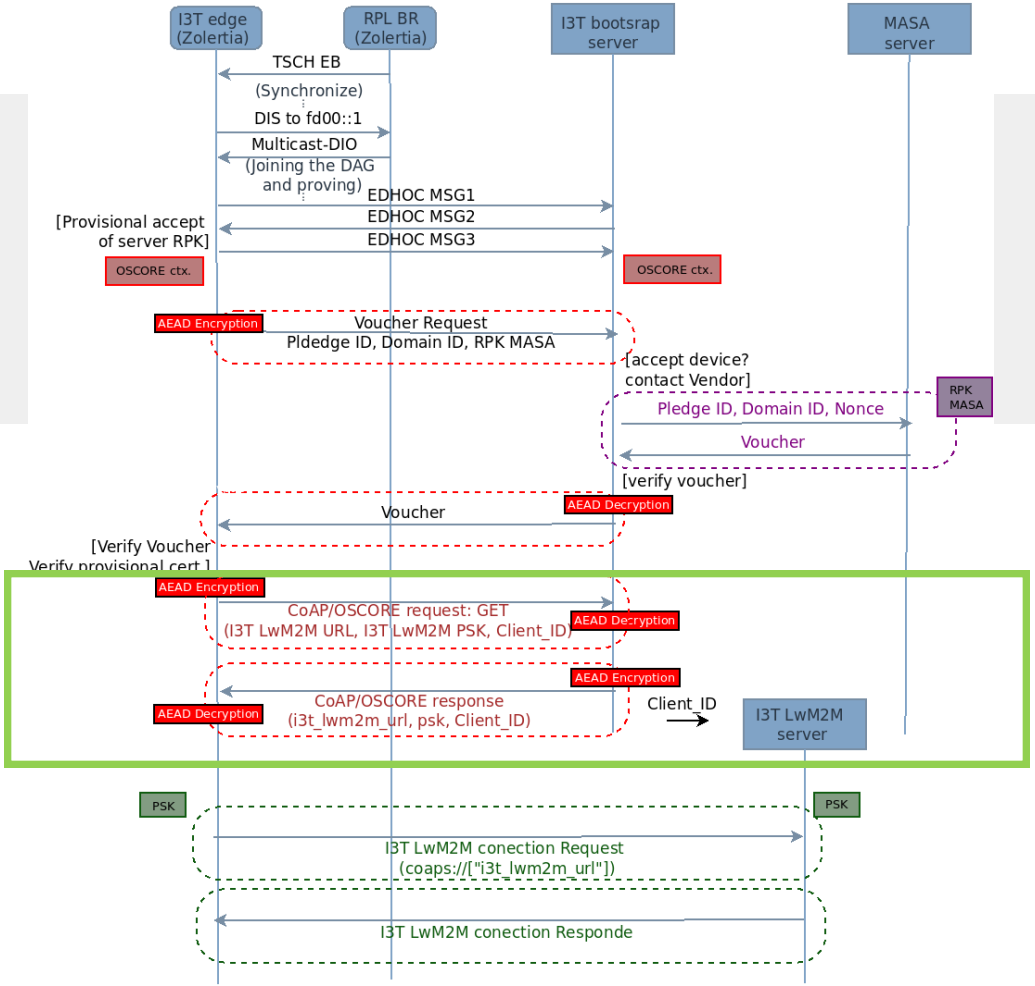
ATHENA Research & Innovation Information Technologies

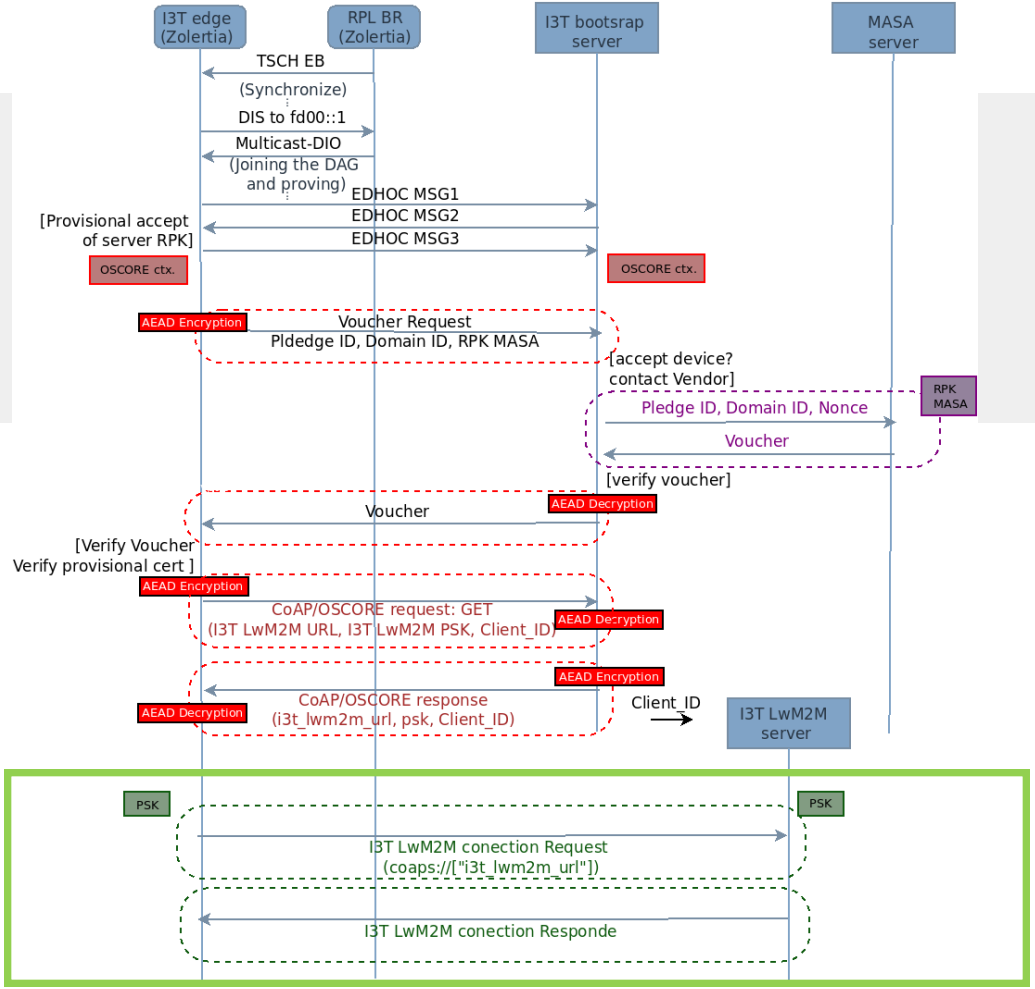
3. Imprint



ATHENA Research & Innovation Information Technologies

4. Enrollment




I3T edge (Zolertia)
RPL BR (Zolertia)
I3T bootsrap server
MASA server
TSCH EB
(Synchronize)
DIS to fd00::1
Multicast-DIO
(Joining the DAG and proving)
EDHOC MSG1
EDHOC MSG2
EDHOC MSG3
[Provisional accept of server RPK]
OSCORE ctx.
OSCORE ctx.
AEAD Encryption
Voucher Request
Pledge ID, Domain ID, RPK MASA
[accept device? contact Vendor]
RPK MASA
Pledge ID, Domain ID, Nonce
Voucher
[verify voucher]
AEAD Decryption
Voucher
[Verify Voucher Verify provisional cert]
AEAD Encryption
CoAP/OSCORE request: GET
(I3T LwM2M URL, I3T LwM2M PSK, Client_ID)
AEAD Decryption
AEAD Encryption
AEAD Decryption
CoAP/OSCORE response
(i3t_lwm2m_url, psk, Client_ID)
Client_ID
I3T LwM2M server
PSK
PSK
I3T LwM2M conection Request
(coaps://["i3t_lwm2m_url"])
I3T LwM2M conection Responde

5. Done

Συμπεράσματα

- Σχεδίαση και υλοποίηση της διαδικασίας αυτόματης εγκατάστασης ενός νέου κόμβου σε βιομηχανικό δίκτυο πραγματικού χρόνου
- Αξιολόγηση της απόδοσης του EDHOC σε δίκτυο που αποτελείται από συσκευές με περιορισμένους πόρους
- Επιτυχημένη δοκιμή σε επίσημα τεστ διαλειτουργικότητας της IETF
- Συμμετοχή στην τρέχουσα φάση ανάπτυξης του σχετικού προτύπου EDHOC σε συναντήσεις με το Lake Working Group της IETF

Ευχαριστώ!